



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/941,553	08/30/2001	Anthony Ioele	CITI0234-US	6102
27510	7590	12/16/2004	EXAMINER	
KILPATRICK STOCKTON LLP 607 14TH STREET, N.W. WASHINGTON, DC 20005			ADAMS, JONATHAN R	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 12/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/941,553

Applicant(s)

IOELE ET AL.

Examiner

Jonathan R Adams

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 August 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) _____ is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 3 and 8-19 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. As to claim(s) 3, 8, and 19:

Claims 3 and 8 recites the limitation "Recording all events happening in the system". It is unclear as to what the applicant means by "all events".

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claim 1, 2 and 7 rejected under 35 U.S.C. 102(a) as being anticipated by Shanklin et al., US Patent No 6578147 (hereafter referred to as '147).

6. As to claim(s) 1:

- '147 teaches using an IDS electronic wall to record and detect intrusions based on access request communication:

- Routing an external access request from the internet to a web site and limiting the external request based on the type of external access / local network 10 could be any system of interconnected computer stations 10a, typically having a server 10b to function as a sort of gateway to network resources. (Col 3, Line 51-54, '147), Internet connections (Col 4, Line 5, '147), If the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection (Col 4, Line 56, '147)
- Providing an electronic wall between the Internet and private network of the web site for receiving/routing external access / The sensor 11 also analyzes each packet's relationship to adjacent and related packets in the data stream. If the analysis indicates misuse, the sensor may act autonomously to take action, such as disconnection (Col 4, Line 56, '147)
- Detecting the routed external access request and determining if the request is an attack / The signatures detected by sensor 11 include those associated with malicious intent attacks, denial of service attacks, evasion attempts, and other methods of misuse. (Cpl 4, Line 39-41), Context-oriented signatures consist of known network service vulnerabilities that can be detected by inspecting packet headers. Examples of context-oriented signatures are SATAN, TCP Hijacking, and IP spoofing signatures (Col 4-5, Lines 64-1, '147)
- Routing the access request within the private network to a particular area of the private network based on a location address / Packets forwarded into the local network (Col 3, Line 30-31, '147)

Art Unit: 2134

- Recording routing of external access request / Specifically, a "copy to" operation is used to send each packet to the appropriate sensor as well as to the destination in local network 10 to which the packet is addressed (Col 6, Line 39-41, '147)

7. As to claim(s) 2:

Electric wall detects access request / detecting unauthorized access on a network as indicated by signature analysis of packet traffic (Col 1, Line 63, '147)

8. As to claim(s) 7:

Primary/secondary means for providing electronic wall / Multiple IDS Sensors (Fig 2, Elements 21, '147)

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 3-5, 8-13, 19 rejected under 35 U.S.C. 103(a) as being unpatentable over '147 in view of Terry Escamilla, "Intrusion Detection"

As to claim(s) 3, 4, 5:

Art Unit: 2134

11. '147 teaches using an IDS electronic wall to record and detect intrusions based on access request communication. '147 does not teach all of the events an IDS is capable of monitoring. Escamilla teaches recording/monitoring a subset of the total range of relevant events (Page 174, Lines 1-7, Escamilla), including access requests (Page 202, Line 15, Escamilla). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the IDS event recording/monitoring details taught by Escamilla in the invention of '147. One of ordinary skill in the art would have been motivated to use the IDS event recording/monitoring details taught by Escamilla in the invention of '147 because Escamilla teaches standard IDS theory and practice for increasing network security.

12. As to claim(s) 8:

First screening of requests from Internet for access to plurality of Internet hosting sites /

Second level of security that detects and prevents unauthorized access to the plurality of Internet hosting sites by access request that are passed by the first level / Third level of security that provides second screening of access requests authorized by second level of security / Multiple IDS Sensors (Fig 2, Elements 21, '147)

Fourth level of security provides recording of events happening in the plurality of Internet hosting sites / recording/monitoring a subset of the total range of relevant events (Page 174, Lines 1-7, Escamilla)

13. As to claim(s) 9:

Art Unit: 2134

First level has plurality of routers that screen the access requests based on a type of each request and route the passed request to the second level / Routers/switches route requests based on IP location type

14. As to claim(s) 19:

Fourth level of security comprises event log manager maintained in a server that connects throughout network of at least one of the plurality of Internet hosting sites and records events happening to hosting site / recording/monitoring a subset of the total range of relevant events (Page 174, Lines 1-7, Escamilla)

As to claim(s) 10:

15. '147 as modified above teaches using an IDS electronic wall to record and detect intrusions based on access request communication by recording/monitoring a subset of the total range of relevant events. '147 as modified above does not teach for the IDS systems of '147 to combined with network firewalls. Escamilla teaches the combination of an IDS with a network firewall (Page 194, Line 5, Escamilla). It would have been obvious to a person of ordinary skill in the art at the time of invention to combine the multiple IDSs in 147 as modified above with network firewalls. One of ordinary skill in the art would have been motivated to combine the multiple IDSs in 147 as modified above with network firewalls because the IDS core logic could be easily combined with a firewall, such as Netranger, to add network IDS capabilities (Page 194, Line 17, Escamilla)

16. As to claim(s) 11:

Load balancing access requests from first level across the plurality of firewall systems /
Packet load balancer (Fig 5, Element 52, '147)

17. As to claim(s) 12, 13:

Second level comprises intrusion detection systems with detection engine in
front/behind firewall / Combined IDS/Firewall series (Fig 3, Elements 31, '147)

18. Claims 6, 14 rejected under 35 U.S.C. 103(a) as being unpatentable over '147 in
view of Kimball et al., US Patent No 5859959 (hereafter referred to as '959).

As to claim(s) 6:

19. '147 teaches using an IDS electronic wall to record and detect intrusions based
on access request communication. '147 does not specifically teach the network
configuration for the local protected network. '959 teaches a redundantly switched
network with multiple redundant switches (Fig 1, '959), (Fig 5, '959). It would have
been obvious to a person of ordinary skill in the art at the time of invention to use the
multiply redundant switching networks taught in '959 in the invention of '147. One of
ordinary skill in the art would have been motivated to use the multiply redundant
switching networks taught in '959 in the invention of '147 because using multiply

Art Unit: 2134

redundant switching networks creates a fault tolerant environment which favorably enhances reliability.

20. As to claim(s) 14:

Third level comprises switches that manage sub-networks within a network for each of the Internet hosting sites / (Fig 1, '959), (Fig 5, '959)

21. Claim 15-18 rejected under 35 U.S.C. 103(a) as being unpatentable over '147 in view of '959 in further view of Sharma et al., US Patent No 6754716 (hereafter referred to as 716).

As to claim(s) 15:

22. '147 as modified above teaches using an IDS electronic wall to record and detect intrusions based on access request communication using redundant routers to deliver data to subnetworks. '147 Does not specifically teach for the routers to maintain a list of addresses of subnetworks to screen/direct access requests. '716 teaches the use of a list of the IP addresses of these authorized devices is stored in each of the network devices (Col 2, Line 29-33, '716). It would have been obvious to a person of ordinary skill in the art at the time of invention to use IP address lists to process/filter data through to subnetworks. One of ordinary skill in the art would have been motivated to use IP address lists to process/filter data through to subnetworks because IP address lists provide a simple logical method for process/filter data through to subnetworks.

23. As to claim(s) 16:

Third level of security comprises a switch for managing a plurality of subnetworks within a network corresponding to Internet hosting site / LAN subnet (Fig 1, Element 104, '716)

24. As to claim(s) 17:

Switch maintains addresses of the sub-networks of the corresponding hosting site and provides the second screening based on the address list of any one of the access requests authorized by second level routed to hosting site / the IP addresses of these authorized devices is stored in each of the network devices (Col 2, Line 29-33, '716)

25. As to claim(s) 18:

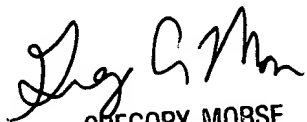
Switch comprises two duplicate switches with a primary and secondary backup switch / Uplink A, Uplink B (Fig 5, Elements 60, 61, '959)

Conclusion

26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (571)272-3832. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

Art Unit: 2134

27. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (571)272-3838. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100